

CLAIMS

1. A method of calculating a value of a given function by using an apparatus including a plurality of computers, comprising:
 - an input process; and
 - an output process,characterized in that the input process inputs a circuit and an input bit to the circuit to the plurality of computers, and
 - one of the computers firstly performs calculation and transmits the calculation result to another computer and the another computer which has received the calculation result performs the next calculation such that calculation is performed by one computer after another, and when all the computers have performed calculation once, the last computer which has performed calculation transmits the calculation result to the first computer which has performed calculation, and after this, calculation is performed by one computer after another and the calculation result is transmitted to the next computer such that the calculation of each cycle is repeated.
2. A method of calculating a value of a given function by using an apparatus including a plurality of computers, comprising:
 - an input process;
 - an ElGamal cipher text preparation process;
 - a sequential substitution reencryption process; and
 - a result output process,characterized in that the input process comprises an information input step of inputting to the plurality of computers information on a circuit including a plurality of gates and information on the plurality of computers, and a dispersion input step of inputting to each of the computers each one of plural pieces of

partial data which are obtained by dispersing input data of the function into plural pieces by the number of the computers,

the ElGamal cipher text preparation process comprises an ElGamal cipher text preparation step of generating a set of ElGamal cipher texts in which at least one of the computers corresponds to the gate of the circuit that realizes the given function,

the sequential substitution reencryption process comprises a step of allowing each of the computers to perform a substitution reencryption process one after another, and the substitution reencryption process comprises a cipher text obtaining step of allowing the computer in this turn to receive the set of ElGamal cipher texts from the computer in the previous turn, a cipher text substitution and reencryption step of changing an order of the set of cipher texts received in the cipher text obtaining step for substitution and subjecting those cipher texts to reencryption, and a step of disclosing the data generated in the cipher text substitution and reencryption step to at least the computer in the next order, and

the result output process comprises a partial decryption step of deciphering or partially deciphering a part of the cipher texts generated in the cipher text substitution and reencryption step, a decryption step of deciphering a cipher text that enciphers data corresponding to the input to the circuit in the cipher texts generated in the cipher text substitution and reencryption step, and an evaluation step of evaluating an output of the circuit by using the data deciphered in the decryption step and the data partially deciphered in the partial decryption step.

3. A calculation system for evaluating a function, comprising:

a plurality of computers;

communication means for performing communication with the plurality of

computers;

input process means;

ElGamal cipher text preparation means;

sequential substitution reencryption means; and

result output means,

characterized in that the input means inputs information on a circuit whose output is desired to be obtained, information on the plurality of computers, and information on which part of an input to the circuit each of the computers has,

the ElGamal cipher text preparation means prepares ElGamal cipher texts for generating a set of ElGamal cipher texts corresponding to gates of the circuit that realizes the given function,

the sequential substitution reencryption means comprises cipher text obtaining means for allowing the computer in this turn to receive the set of ElGamal cipher texts from the computer in the previous turn, cipher text substitution and reencryption means for changing an order of the set of cipher texts received by the cipher text obtaining means for substitution and subjecting those cipher texts to reencryption, and means for disclosing the data generated by the cipher text substitution and reencryption means to at least the computer in the next order, and

the result output means comprises partial decryption means for deciphering or partially deciphering a part of the cipher texts generated by the cipher text substitution and reencryption means, decryption means for deciphering encryption related to itself of a cipher text that enciphers data corresponding to the input to the circuit in the cipher texts generated by the cipher text substitution and reencryption means, and evaluation means for evaluating an output of the circuit while using the data deciphered by the decryption means by the plurality of computers and the data partially deciphered by the partial decryption means by the plurality of computers.

4. The calculation method according to Claim 2,
 characterized in that the set of ElGamal cipher texts corresponding to each of the gates is a set of ElGamal cipher texts of a secret key generated corresponding to each of the gate by each of the computers, and
 a public key used for generating the ElGamal cipher texts is a sum of public keys corresponding to gates for generating two signals input to this gate.

5. The calculation method according to Claim 2,
 characterized in that the input process further comprises a step of inputting an area variable of an ElGamal encryption method to each of the computers,
 the ElGamal cipher text preparation process further comprises a gate secret key generating step of generating a secret key of the ElGamal cipher texts corresponding to each of the gates of the circuit by each of the computers,
 each of the computers performs:
 a gate public key generating step of generating a gate public key corresponding to the secret key generated in the gate secret key generating step;
 a gate public key validity proof generating step of generating a gate public key validity proof for the public key generated in the gate public key generating step;
 a gate public key validity proof disclosing step of disclosing the gate public key validity proof generated in the gate public key validity proof generating step;
 an input gate secret key generating step of generating a secret key of the ElGamal cipher texts corresponding to a gate where an input is directly made to the circuit of the gates of the circuit;
 an input gate public key generating step of generating an input gate public key corresponding to the secret key generated in the input gate secret key generating step;

an input gate public key validity proof generating step of generating a validity proof for the public key generated in the input gate public key generating step;

an input gate public key validity proof disclosing step of disclosing the input public key validity proof generated in the input gate public key validity proof generating step;

a gate public key obtaining step of obtaining gate public keys generated by other respective computers;

a gate public key integration step of integrating the gate public keys obtained in the gate public key obtaining step;

a gate public key encryption step of enciphering the gate secret key generated by this computer with the gate public key integrated in the gate public key integration step;

a gate secret key cipher text disclosing step of disclosing a gate secret key cipher text generated in the gate public key encryption step;

a gate secret key cipher text validity proof generating step of generating a validity proof for the gate secret key cipher text;

a gate secret key cipher text validity proof disclosing step of disclosing the gate secret key cipher text validity proof generated in the gate secret key cipher text validity proof generating step;

an input cipher text generating step of generating a cipher text corresponding to a part of the input of the circuit input to each of the computers.

an input cipher text validity proof generating step of generating a validity proof for the cipher text corresponding to the part of the input of the circuit generated in the input cipher text generating step;

an input cipher text validity proof disclosing step of disclosing the proof generated in the input cipher text validity proof generating step; and

an output cipher text generating step of generating and disclosing a cipher

text corresponding to an output of the gate,

the sequential substitution reencryption process comprises:

a gate secret key cipher text substitution and reencryption step of changing an order of a set of the gate secret key cipher texts with one substitution randomly selected on the basis of a predetermined permitted substitution method for reencryption;

an input cipher text substitution and reencryption step of changing an order of a set of the input cipher texts with one substitution randomly selected on the basis of a predetermined permitted substitution method for reencryption;

an output cipher text substitution and reencryption step of changing an order of a set of the output cipher texts with one substitution randomly selected on the basis of a predetermined permitted substitution method for reencryption; and

a gate secret key cipher text, input cipher text, and output cipher text substitution and reencryption validity proof generating and disclosing step of generating and disclosing validity proofs for the substitution and reencryption performed in the gate secret key cipher text substitution and reencryption step, the input cipher text substitution and reencryption step, and the output cipher text substitution and reencryption step,

the partial decryption step of the result output process comprises:

a gate secret key partial decryption step of partially deciphering the gate secret key cipher texts by mutually performing communication and calculation by the computers;

an input cipher text partial decryption step of partially deciphering the input cipher texts by mutually performing communication and calculation by the computers;

an output cipher text partial decryption step of partially deciphering the output cipher texts by mutually performing communication and calculation by the

computers; and

a gate secret key, input cipher text, and output cipher text partial decryption step validity proof generating and disclosing step of generating and disclosing the validity proofs for the partial decryption performed in the gate secret key partial decryption step, the input cipher text partial decryption step, and the output cipher text partial decryption step, and

the calculation method further comprises a step of verifying various validity proofs disclosed by other computers.

6. A calculation system, comprising a plurality of computers, input means, and output means, in which one of the computers firstly performs calculation and transmits the calculation result to another computer and the another computer which has received the calculation result performs the next calculation such that calculation is performed by one computer after another, and when all the computers have performed calculation once, the last computer which has performed calculation transmits the calculation result to the first computer which has performed calculation, and after this, calculation is performed by one computer after another and the calculation result is transmitted to the next computer such that the calculation of each cycle is repeated,

characterized in that the input means inputs information on a circuit and a part of input bits to the circuit to the computer,

the calculation of the zero-th cycle is performed before the first computer performs the calculation of the first cycle,

the plurality of computers comprise data obtaining means for obtaining transmitted data used in the calculation of each cycle, validity proof verifying means, signature text verifying means, first computer special calculating means performed by the first computer, random number generating means for performing random number generation, a main calculation calculating means for

performing a main calculation, validity proof generating means for proving a validity for a calculation performed in the main calculation, signature means, and data transmission means,

the transmitted data comprises data transmitted from other computer, data main body, a validity proof for the data main body, and a signature text,

the signature text comprises data including a signature text corresponding to a combination of the data transmitted from the other computer, the data main body, and the validity proof for the data main body,

the validity proof verifying means verifies a validity proof in the transmitted data

the signature text verifying means verifies the signature text in the transmitted data,

the main calculation calculates the random number generated by the random number generating means,

the signature means generates a signature text for a combination of the transmitted data, the data main body that is the calculation result calculated in the main calculation, and the validity proof generated by the validity proof generating means, and

the data transmission means transmits a combination of the transmitted data, the data main body that is the calculation result calculated in the main calculation, the validity proof generated by the validity proof generating means, and the signature text generated by the signature means.

7. The calculation system according to Claim 6, wherein a data main body of the transmitted data and the data main body that is the calculation result calculated in the main calculation comprise a combination of multiple sequence alignment ElGamal cipher texts on a true value group ring and extended multiple sequence alignment ElGamal cipher texts on the true value group ring in the

calculation of the first cycle.

8. The calculation system according to Claim 7, characterized in that the calculation of each cycle comprises calculation means for the first cycle and calculation means of cycles subsequent to the first cycle,

the calculation means generates the combination of the multiple sequence alignment ElGamal cipher texts on the true value group ring and the extended multiple sequence alignment ElGamal cipher texts on the true value group ring with the calculation means of the zero-th cycle and comprises reencryption public key generating means for generating a public key used for reencryption by the calculation means of the first cycle, data conversion means for converting the transmitted data, secret key conversion means, and random number conversion means,

the data conversion means is adapted to convert the combination of the cipher texts that are the data main body with another combination of multiple sequence alignment ElGamal cipher texts on the true value group ring and extended multiple sequence alignment ElGamal cipher texts on the true value group ring,

the secret key conversion means converts the secret key used for the combination of the cipher texts that are the calculation result of the data conversion means with a secret key corresponding to the public key generated by the reencryption public key generating means,

the calculation result of the secret key conversion means comprises a combination of multiple sequence alignment ElGamal cipher texts on the true value group ring and extended multiple sequence alignment ElGamal cipher texts on the true value group ring,

the random number conversion means is adapted to convert a random number used for the combination of the cipher texts that are the calculation

results of the data conversion means, and

the calculation result of the random number conversion means comprises a combination of multiple sequence alignment ElGamal cipher texts on the true value group ring and extended multiple sequence alignment ElGamal cipher texts on the true value group ring.

9. The calculation system according to Claim 8, characterized in that the calculation means of the cycles subsequent to the first cycle comprises of the calculation means of the second cycles and the calculation means of cycles subsequent to the second cycle,

the data main body of the transmitted data and the data main body calculated in the main calculation comprise a combination of multiple sequence alignment ElGamal cipher texts on the true value group ring and extended multiple sequence alignment ElGamal cipher texts on the true value group ring in the second calculation, and

the calculation means of the second cycles cipher text conversion means for converting the data main body of the transmitted data to generate an ElGamal cipher text or an ellipse curve ElGamal cipher text and partial decryption means for partially deciphering the cipher texts of the data main body of the transmitted data.

10. The calculation system according to Claim 9, characterized in that the calculation means of the cycles subsequent to the second cycle only comprises the calculation means of the third cycle,

the calculation means of the third cycle of the main calculation means outputs the transmitted data as it is, and

the validity proof generating means outputs a null string.